Sub B2

21. (New) A computing environment configured to process a trusted command, comprising:

an untrusted environment to parse a trusted command; and

a trusted environment to receive the trusted command from the untrusted environment and to communicate a representation of the trusted command.

22. (New) The computing environment of claim 21, wherein the trusted environment executes the trusted command if the trusted environment detects confirmation of the trusted command.

23. (New) The computing environment of claim 21, wherein the representation of the trusted command is communicated through a trusted path.

A1 cont

24. (New) The computing environment of claim 23, wherein the trusted path is between a user and the trust environment.

25. (New) The computing environment of claim 21, further comprising:

a user interface to communicate with the untrusted environment and the trusted environment.

26. (New) A method of processing a trusted command, comprising the steps of:

parsing a trusted command in an untrusted mode of a system;

establishing a trusted mode of the system; and

communicating a representation of the trusted command in the trusted mode.

27. (New) The method of claim 26, further comprising the step of:

executing the trusted command in the trusted mode if confirmation of the trusted command is detected.

28. (New) The method of claim 26, the communicating step comprising the step of:

displaying a representation of the trusted command.

29. (New) A method of processing a trusted command, comprising the steps of:

interpreting a trusted command in an untrusted mode; and

executing the trusted command in a trusted mode.

30. (New) The method of claim 29, further comprising the step of:

communicating a representation of the trusted command in the trusted mode.

B2

31. (New) The method of claim 30, further comprising the step of:

verifying the trusted command in the trusted mode after the communicating step.

A1 Cn't

32. (New) The method of claim 31, the verifying step comprising the step of:

requesting confirmation of the trusted command in the trusted mode.

33. (New) The method of claim 29, further comprising the step of:

using the trusted command in the untrusted mode.

34. (New) The method of claim 29, further comprising the step of:

transitioning from the untrusted mode to the trusted mode.

35. (New) The method of claim 29, further comprising the step of:

transitioning from the untrusted mode to the untrusted mode.

36. (New) The method of claim 35, further comprising the step of:

issuing a message to indicate a transition to the untrusted mode before the transitioning step.

37. (New) The method of claim 29, further comprising the step of:

detecting if a command is a trusted command in an untrusted mode.

38. (New) A machine-executed method for executing a trusted command issued by a user on a computing system including an untrusted computing environment and a trusted computing environment, said method comprising the steps of:

(a) receiving user identification data in the trusted computing environment from the user via a trusted path;

(b) receiving the trusted command from the user in the trusted computing environment via an untrusted path;

(c) parsing the trusted command in the untrusted computing environment to generate a parsed command;

B2

(d) submitting the parsed command to the trusted computing environment;

(e) performing a security check on the parsed command and user identification data in the trusted computing environment; and

A1 cont.

(f) executing the trusted command in the trusted computing environment.

39. (New) The method of claim 38, wherein the security check enforces a security criterion from the Department of Defense Trusted Computer System Evaluation Criteria (Ref. No. DOD 5200.28-STD).

40. (New) A method including the steps of claim 38 and additionally including the steps, executed after step (d) and before step (f) of claim 38, of:

(1) in the trusted environment, displaying a representation of the parsed command to the user;

(2) receiving a signal from the user signifying whether the displayed representation accurately represents the trusted command; and

(3) if the signal signifies that the displayed representation does not accurately represent the trusted command, then preventing the performance of step (f) of claim 38.